INTERNAL AUDIT REPORT

Review of Information Protection

Fairfax County Internal Audit Office

TABLE OF CONTENTS

Introduction

The County established the Information Technology Advisory Group (ITAG) in 1993 to investigate the state of the County's Information Technology (IT) program. ITAG made nine policy recommendations and twelve technical recommendations. Two of the policy recommendations addressed centralizing the security function in the Department of Information Technology (DIT), and documenting the disaster recovery and business resumption between DIT and the departments that are "adopted, supported, tested, maintained, and properly funded". One of the technical recommendations suggested that an appointed individual develop and control security standards for software development in both mainframe and departmental distributed systems. In addition, the County has adopted ten IT Fundamental principles to achieve the County's business goals through the use of information technology. One of these principles emphasizes the importance that management places on information protection, which is similar to protecting other County resources, such as money, physical assets, or employees.

Information is a critical asset that supports the mission of the County. The Information Protection Program was implemented in the County to ensure an acceptable level of risk as defined by management. This program focuses on centralized control with decentralized activities at the individual department level. The Information Protection Branch in DIT administers the oversight of this program. Departments are required to comply with the County's Information Protection Manual through their own designated Information Protection Coordinators. The Information Protection Manual contains guidelines and standards that apply to all County employees, vendors, and contractors to ensure the *confidentiality, integrity*, and *availability* of County information resources. The Information Protection Branch has four (4) Information Security Analysts, and there are approximately seventy-five (75) Information Protection Coordinators in the County departments.

Purpose and Scope

This audit was performed as part of our FY 2001 Long-Range Audit Plan. The purpose of securing information is to protect the County's interests and support DIT's mission to "deliver quality and innovative information technology solutions to provide citizens, the business community, and County staff with convenient access to appropriate information and services". Our audit objective was to determine the adequacy of the County's current computer security function by evaluating the planned and existing control objectives, dissemination of policies, and compliance with these policies.

Methodology

Our review included interviewing appropriate County employees from the Department of Information Technology who are involved with protecting information. The audit included testing for compliance with the County's Information Protection Manual. We also conducted a survey of the Information Protection Coordinators in each department to determine their compliance with the County's Information Protection Manual. We shared the results of the survey with DIT management.

This audit was performed in accordance with the Government Accounting Office's (GAO) generally accepted government auditing standards and the GAO Standards of the Federal Information System Controls Audit Manual (January 1999). This manual contains a Best Practices Model of eight nonfederal leading organizations recognized as having strong information security programs. We used this model to determine the County's compliance. The model includes the five risk management principles to:

1. assess risk and determine needs,
2. establish a central management focal point,
3. implement appropriate policies and related controls,
4. promote awareness, and
5. monitor and evaluate policy and control effectiveness.

Executive Summary

In our opinion, the County's Information Protection program meets some, but not all of the computer security best practices based on the U.S. GAO Standards of the Federal Information System Controls Audit Manual. In addition, some requirements of the County's program are not being met. This audit was performed during a time when DIT was in the process of improving the County's network security through a self-initiated vulnerability assessment conducted by an external security vendor. The following are identified as areas where security functions and documentation need to be improved:

- Documents regarding the County's Business Continuity and Disaster Recovery need to be reviewed, updated, and distributed in a timely manner.

- The County should have a documented incident handling program to effectively and efficiently address any breach in system security that may affect data availability, integrity, and confidentiality.

- The network security policy should be updated to guide DIT in the administration and maintenance of the County's network infrastructure.

- The Information Protection Branch should monitor department compliance to the Information Protection Manual.

- The Information Protection Branch should participate in reviewing security controls of all the County's new computer system development efforts.

Certain security related information has been omitted from general disclosure. This information would, if disclosed, subject the County to potential system vulnerabilities and disruptions.

Comments and Recommendations

1. DIT does not have an up-to-date Business Impact Analysis (BIA), Business Continuity Plan (BCP), and the disaster recovery related data captured in the Living Disaster Recovery Planning System (LDRPS).

The BIA was developed for the Data Center in April 1996. The focus of this document was mainframe based and a survey of the departments was conducted that was voluntary in nature. The BCP replaces the outdated Disaster Recovery Plan. This document was developed for the Data Center in June 1998. Neither has been updated since they were developed. Like the BIA, the BCP focuses on "essential mainframe computer support" according to its purpose statement.

The BCP requires at least semi-annual disaster recovery exercises. DIT has successfully conducted their exercises at the hot site in Philadelphia. The last three disaster recovery tests occurred quarterly in March and June 2000 and January 2001. The January 2001 exercise covered mainframe and non-mainframe based applications of all major systems in Public Safety, Department of Finance, Department of Public Works, Department of Planning & Zoning, and the Department of Human Resources.

The disaster recovery related data (known as dictionaries) are captured in the LDRPS software. The dictionaries include names of employees, vendors, critical systems and their ratings, and other pertinent information to assist management in case of a disruption. These dictionaries were updated in either September 1999 or September 2000.

The County's Information Protection Manual states that each *department* should conduct a business impact analysis annually. The same section requires that the *departments* review the plans of the data custodian (i.e. DIT) to ensure that their needs are met. It also states that "all continuity plans should be reviewed, updated and tested annually". DIT is required to update the BCP quarterly according to the plan itself. The same plan requires the LDRPS to be updated quarterly. In addition, industry best practices under the GAO Principles for Managing an Information Security Program states that an organization should "Assess Risk and Determine Needs" on a continuing basis by developing and updating documents like the BIA, BCP, and the LDRPS dictionaries.
The scope of the BCP and the Disaster Recovery Plan is different. The BCP only deals with critical operations needed to continue working after an unplanned incident. The BCP addresses minimum requirements to provide services to the customers or clients. The Disaster Recovery Plan defines all needed actions to restore to normal operation after an unplanned incident. The Disaster Recovery Plan recovers all operations.

The County will not be fully prepared to identify and restore critical and non-critical systems in a timely manner in case of an unplanned event without a sound Information Protection Program that assesses risk and determines business needs on a continuing basis. Therefore, the business needs of the departments may not be met.

DIT has established a solid foundation by developing the initial BIA and BCP, and purchasing the LDRPS software to address business continuity issues in the County. However, the two documents and the LDRPS software have not been updated to protect data and meet department needs in case of a disruption.

Recommendation 1a Medium Priority

We recommend DIT update their BIA originally developed in April 1996. The BIA document provides the basis for justifying the Information Protection Program and assigning priorities to the security measures to be implemented and should be reviewed and updated annually. The scope of the BIA should include support for mainframe and non-mainframe applications. All departments should respond in order to fairly assess their business needs in case of a disruption.

Department Response

DIT will review the County's BIA and update as required. This update will require extensive involvement of business area system managers within agencies and departments. DIT will develop a plan for a project to update the BIA that will be coordinated through agency directors to ensure adequate business analysis. The Information Security Officer will provide a plan of action and identify resources needed to review and update the new plan annually.

Recommendation 1b Medium Priority

We recommend DIT update their BCP developed in June 1998. In addition, DIT should assist the departments with (1) identifying and prioritizing their critical data and operations, (2) identifying resources (hardware, software, system documentation, telecommunications, office facilities and supplies, and human resources) to support critical operations, and (3) establishing the emergency processing priorities and data backup and retention requirements. Since the BCP replaces the Disaster Recovery Plan, the BCP should include the components of both plans.

Department Response

DIT will update its Business Continuity Plan (aka: The Enterprise Operation Center Disaster Recovery Plan) in conjunction with the BIA update (see above). Agencies will be responsible for developing plans to conduct business during unplanned outages of the EOC or other outages of the IT infrastructure.

Recommendation 1c Medium Priority

We recommend DIT update the dictionaries in the LDRPS software that captures disaster recovery related information. The LDRPS should be updated at least quarterly according to the Business Continuity Plan document. The updated information regarding the employee and vendor contacts and critical systems to restore would facilitate the coordination in case of a disruption.

Department Response

DIT will develop a work plan in conjunction with the BCP update.

2. DIT has no documented incident response program to effectively address common security incidents such as those caused by email viruses, other malicious codes (e.g. Trojan horses and worms), and system intruders (hackers) breaching the network.

Generally, a response to a security incident in the County is reactive in nature where management forms an ad hoc team of technical staff to address the problem and later disbands the team. There is no incident response team to initially assess a security incident for immediate handling or through escalation methods as appropriate. There is no plan of action to guide the team that will define strategies and assign roles for responding to the various types of incidents.

Industry best practices under the GAO Principles for Managing an Information Security Program states that an organization should "Establish A Central Management Focal Point" by establishing a computer incident response capability, and, in some cases, serving as members of the Emergency Response Team. The Business Continuity Plan defines the County's Emergency Response Team as the Administration Team. Another GAO Principle requires "Monitoring and Evaluating Policy and Control Effectiveness" to account for and analyze security incidents. This analysis should show increases and decreases in incident frequency, trends, and the status of resolution efforts. This analysis (1) identifies emerging problems, (2) assesses the effectiveness of current policies and awareness efforts, (3) determines the need for stepped up education or new controls to address problem areas, and (4) monitors the status of investigative actions to ensure that no individual incident is dropped and the incidents are handled consistently. Incident handling is closely related to contingency planning as well as support and operations. An incident handling capability may be viewed as a component of contingency planning because it provides the ability to react quickly and efficiently to disruptions in normal processing.

DIT will not be able to respond to security incidents in an efficient and effective manner without an appropriate incident-handling program that is documented, tested, approved, and supported by senior management. Corrective measures were taken in the past to address security incidents as they occurred. For example, in the case of the love virus, DIT responded in a reactive mode. The preferred method is based on a well-planned, deliberate, and proactive approach.

Recommendation 2a Medium Priority

We recommend DIT document a formal incident handling program that would respond to violation or breakdown of security. Incident handling can be considered that portion of the County's business contingency planning that responds to malicious technical threats. An incident response team should be formed that consists of individuals from DIT and other departments. This enhances internal communications and the readiness of the County and better organizes department management to prepare for and respond to incidents. The makeup of the team may include technical and non-technical staff. A response plan for different scenarios should be developed that defines the actions needed based on the types of incidents.

Department Response

DIT will document the current incident handling procedures and practices. The Information Security Officer will gather and document all currently existing practices and procedures. Current procedures and practices will be examined and if additional practices and procedures are required, they will be included.

Recommendation 2b Medium Priority

We also recommend that for each security incident, a summary should detail the incident, how it was discovered, corrective action(s) taken, what monitoring mechanism, if any, was in place at the time, and what was learned. The DIT can measure the frequency of various types of violations as well as conduct a damage assessment by keeping summary records of actual security incidents. This information is helpful to continuously assess the County's security risk and update its security policy.

Department Response

We will investigate the use of our in-house help desk software (Quintus) to track security incidents to a practical level of feasibility within current resources.

The Information Security Officer will develop and publish an incident-handling policy (Procedural Memorandum) by April 2002.

3. The County's Information Protection Program requires an update to the network security policy to support adopting specific procedures and technical controls.

The County's policy addresses at least two of the eight network standards regarding 1) network security mechanism, and 2) network traffic through the following available documents:

- Information Protection Manual
- Procedural Memorandum 70-01
- Procedural Memorandum 70-04
- DIT Memorandum dated June 9, 1995
- Draft Firewall Policy

However, there are additional standards that directly influence design, configuration, installation, management, and maintenance. These services define what will be allowed or denied from the network and how they will be used to meet the business needs.

Industry best practices under the GAO Principles for Managing an Information Security Program states that an organization should "Implement Appropriate Policies and Related Controls". Written policy defines and communicates management requirements and it is based on the implementation of three basic security goals:

- Confidentiality – ensuring that sensitive data is read only by authorized persons
- Integrity – protecting data or software from improper modification, and
- Availability – ensuring that systems, networks, applications and data are online and accessible when needed

A network security policy may contain some or all of the eight (8) network standards:

1. <u>Network risk assessment</u> should be conducted annually by evaluating potential vulnerabilities and threats.
2. <u>Network configuration management</u> should be reviewed when the network malfunctions, or is replaced, repaired, or scheduled for periodic maintenance.
3. <u>Network access security</u> should be restricted to a specific time of the day and weekends

with automatic time zone adjustment.

4. Network security mechanism should protect data through encryption, digital signature, and authentication methods that is either user-based, token-based, biometrics, or a combination of all three methods.

5. Network change management should be documented, tested, and approved either manually or via automated log.

6. Network traffic should be continuously monitored from the County's current computing infrastructure (desktop workstations, LAN servers, network protocols, application software, operating system, database management, and etc.), middleware (client/server), ports, routers, and firewall logs through the use of tools that can help accomplish this task.

7. Security perimeter defense should be setup as an early-warning system to detect and prevent intrusions.

8. Network contingency plan should consider (1) incident response, (2) backup operations, and (3) recovery plans.

The County has a significant risk associated with not having a defined network security policy implemented to appropriately address the security concerns of their current interconnected computing environment. These risks include but are not limited to unauthorized access, computer viruses, Trojan horses (malicious codes), packet (data transmission) sniffing activities, and denial of service. It's difficult to link the need for a network security policy to business risks without an on-going risk assessment mechanism in place. This policy has not been updated in the County.

Recommendation 3a **Medium Priority**

We recommend DIT update the County's network security policy in partnership between the Information Protection Branch, Data Communications Services responsible for network administration, County departments, and external consultant services as necessary. Internal Audit may also be consulted. Although a separate network security policy is preferred, it is acceptable to update existing policies that cover some of the network standards.

Department Response

A separate Network Security Policy will be developed and documented. Information Security Officer will coordinate with Network Manager, and other appropriate staffs, to develop, document and implement policy, procedures and practices. Policy will be written by Mar 2002. Procedures and practices will be identified and documented by May 2002.

Recommendation 3b Medium Priority

The network security policy should consider some of the standards mentioned above. The responsibilities for implementing the network policy may involve a team that includes the security manager, network manager, selected department managers and technical staff from DIT.

Department Response

We are working on formalizing communications between Information security and network teams and our newly created infrastructure and applications architects in updating network security policy.

Recommendation 3c Medium Priority

DIT should establish a project plan for implementation of the updated network policy. This policy should be approved by the County Information Officer.

Department Response

After establishment of a Network Security Policy, the network manager will work with the Security Officer to develop an implementation plan and submit it to the DIT Director and the CIO for approval.

4. The Information Protection Branch does not actively monitor County department compliance to the Information Protection Manual developed in May 1999.

The IP Manual was approved by the County's CIO in May 1999. This is a thorough document that provides guidance to departments regarding the protection of the County's information. The IP Manual will be implemented over a period of time through a "phased-in-approach" with assistance from the Information Protection Branch staff. Furthermore, the IP Manual is a "dynamic" document maintained by the Information Security Manager. Information Protection Branch is not monitoring department compliance to the IP Manual. A survey of the department Information Protection Coordinators shows that while 73% of the respondents know their responsibilities, none of them were performing all of their security duties. According to our survey, between 50 and 75% of the Information Protection Coordinators do not perform specific tasks required by the IP Manual.

The County's IP Manual states that the Information Security Manager is responsible for the "publishing of information protection standards, guidelines and procedures; and monitoring of daily information protection activities and operations to ensure actions are in compliance with criteria contained within the IP Manual". The IP Manual further states that the Information Security Manager will "monitor each agency's progress and provide status reports to the CIO." In addition, Industry best practices under the GAO Principles for Managing an Information Security Program states that a policy should be "Monitored and Evaluated for Control Effectiveness". Monitoring is an important detective control for identifying compliance to established standards and to minimize security breaches, abuse of privileges, and other security concerns.

There is a lack of consistent security practices across the County. There is no monitoring mechanism to determine department compliance to the IP Manual. The worse case scenario is that some departments may not have security controls in place to protect information. The Information Protection Branch has not monitored County departments due to other responsibilities. These include RACF and remote access administration, conducting security awareness training, and providing security advice to County staff.

Recommendation 4 Medium Priority

The Information Protection Branch should monitor all departments' compliance to the IP Manual. This monitoring should be ongoing and cover all departments over a period of time. Information Protection Branch monitoring should focus on the responsibilities of the department heads and the Information Protection Coordinators based on sections 2.4 and 2.5 of the IP Manual. At a minimum, a record of each visit to the departments should be documented as to how the security issues were addressed and resolved. The Information Protection Branch may use this information in follow-up visits to determine department compliance to the IP Manual.

Department Response

The Information Security Officer will continue working with Agency Information Protection Coordinators and will work to increase the awareness and importance of implementing the IPM. The Security Officer will work with the Coordinators to periodically spot-check agencies. Such activity will be documented. To monitor more thoroughly or aggressively will require additional resources. Current resources of the Information Protection Branch are completely committed to daily operations and additional tasking of monitoring compliance with the IPM cannot be accomplished without additional resources. A request for an additional position (Information Security Analyst II) will be submitted along with a request for additional funds to increase use of outside consultant services.

5. The Information Protection Branch is not actively involved in the development of the County's computer system.

There are over 40 ongoing information technology projects that are supported under Fund 104 – Information Technology. The Information Protection Branch participated in some of the development of these in-house and commercial off-the-shelf (COTS) systems on a limited basis. The IP Manual section entitled "Implementation/Responsibilities" defines the responsibilities of the Data Custodian. It states, among other things, the Data Custodian is responsible for "implementing procedural safeguards and cost-effective controls." This responsibility starts at the early stage of computer system development. In addition, industry best practices under the GAO Principles for Managing an Information Security Program states that an organization should "Establish A Central Management Focal Point" by designating a central security group to participate in the early stages of software development projects and test the system to ensure that security implications are addressed.

Adequate security controls may not be available to ensure the protection of information. The cost to add security controls after the original implementation of the computer system is greater than when the security provisions are built in during the early stages of system development.

Recommendation 5 Medium Priority

DIT Information Protection Branch should be involved in the early planning stages of the County's computer system development. In particular, Information Protection Branch staff should participate in the design phase of system development to identify the security-related controls needed to strengthen the protection of information. At a minimum, Project Managers who are responsible for enhancing existing computer systems or implementing new computer systems should be required to route security-related requirements and controls to the Information Protection Branch for review, comments, and recommendations.

Department Response

The Information Security Officer will work closely with the IT Project or Program Manager and other appropriate staff to review all submitted proposals and approved proposals. The Security Officer will work with the IT Portfolio Manager to ensure that security standards are being considered as an integral part of the IT planning process. The Information Security staff will consult with designated Project Managers to ensure that security specifications outlined in the Application Life Cycles Standards (ACLS) are included in all development activities. In addition, the Security Officer will work with the Portfolio Manager and appropriate training staff to include Information Protection training in the DIT Project Managers' course. Security Officer will also examine current processes in place to identify methods needed to have Information Protection involved in the early planning of the County's computer system development. A plan will be developed and submitted to the DIT Director in July 2002.